A Practical Approach To **Cyber Security**

WCA - 2019

Google Cloud

Home sales are held up; Baltim

https://www.baltimoresun.com/news/maryland...

SECTIONS

THE BALTIMORE SUN

SUBSCRIBE 4 weeks for 99¢

LOG IN

FRIDAY MAY 17, 2019

LATEST ENEWSPAPER PREAKNESS ASK US PROMS MARYLAND POPULAR SPORTS

70°

ADVERTISEMENT

News / Maryland / Baltimore City

Home sales are held up; Baltimore ransomware attack cripples systems vital to real estate deals

Ada County Highway District fa

https://www.idahostatesman...

Idaho Statesman

BOISE & GARDEN CITY

This Ada County agency just suffered a ransomware attack. Now the FBI is investigating

BY HAYLEY HARDING

MAY 15, 2019 12:26 PM, UPDATED MAY 15, 2019 12:31 PM

Waiting for securepubads.g.doubleclick.n...

consumable

Ryuk malware hacked a county

https://www.latimes.com/local/lanow/la-me-imperial-county-website-down-...

TOPICS SEARCH

Los Angeles Times

SUBSCRIBE 4 weeks for only 99¢

LOG IN

F-16 military fighter jet crashes into building in Southern California

Disneyland, dozens of cities could be flooded by dam failure from huge storm,...

Homeless population jumps by thousands across the San Francisco Bay Area

Trump and Biden, poter 2020 rivals, both head Pennsylvania, a key...

L.A. NOW LOCAL

Ryuk malware hacked a county government website. It's been down for 6 days

Crippling ransomware attacks

https://www.cnn.com/2019/05/10/politics/ransomware-attacks-us-cities/in...

CNN politics

45 CONGRESS SUPREME COURT FACTS FIRST 2020 ELECTION

Crippling ransomware attacks targeting US cities on the rise

By Kevin Collier, CNN

Updated 10:34 PM ET, Fri May 10, 2019


1
BILLION
users
YouTube

Let’s level set with some

Definitions and Examples

Cyber Security

Protecting digital data and assets (a subset of information security)

InfoSec Elements

1. Confidentiality
2. Integrity
3. Availability

Types of Attackers

1. Activists
2. Profiteers
3. Nation States

Common Attacks

1. Data Exfiltration
2. Ransomware
3. Advanced Persistent Threats

Typical View of Security

Traditional Security

As you conduct periodic assessments of risk, here are

Five Things to Consider

Google Cloud

Use Policy to Limit Access

- Least privilege access is imperative
- Focus on central administration and monitoring
- Regularly audit your accounts and review access privileges

Protect the Logs

- Compromise of logs can lead to a complete systems compromise
- Know where your logs are being stored and who can access them
- Consolidate and retain your logs for as long as possible

Understand Your Network Boundaries

- Connections to the cloud open new attack vectors for your network
- Define a connectivity strategy to the cloud from on-premises
- Options: Trusted Internet Connections, Virtual Private Cloud, etc

Inventory Your Endpoints

- Build and maintain an inventory of your endpoints
- Understand your endpoint statuses (patched, virus scanned, etc)
- Employ a rules engine that grants access based on status

Patch, Patch, Patch

- Patch your systems as soon as patches are available
- Make sure your providers are patching their services
- Get out of the patching business where able

A view of the Google's cyber security landscape from

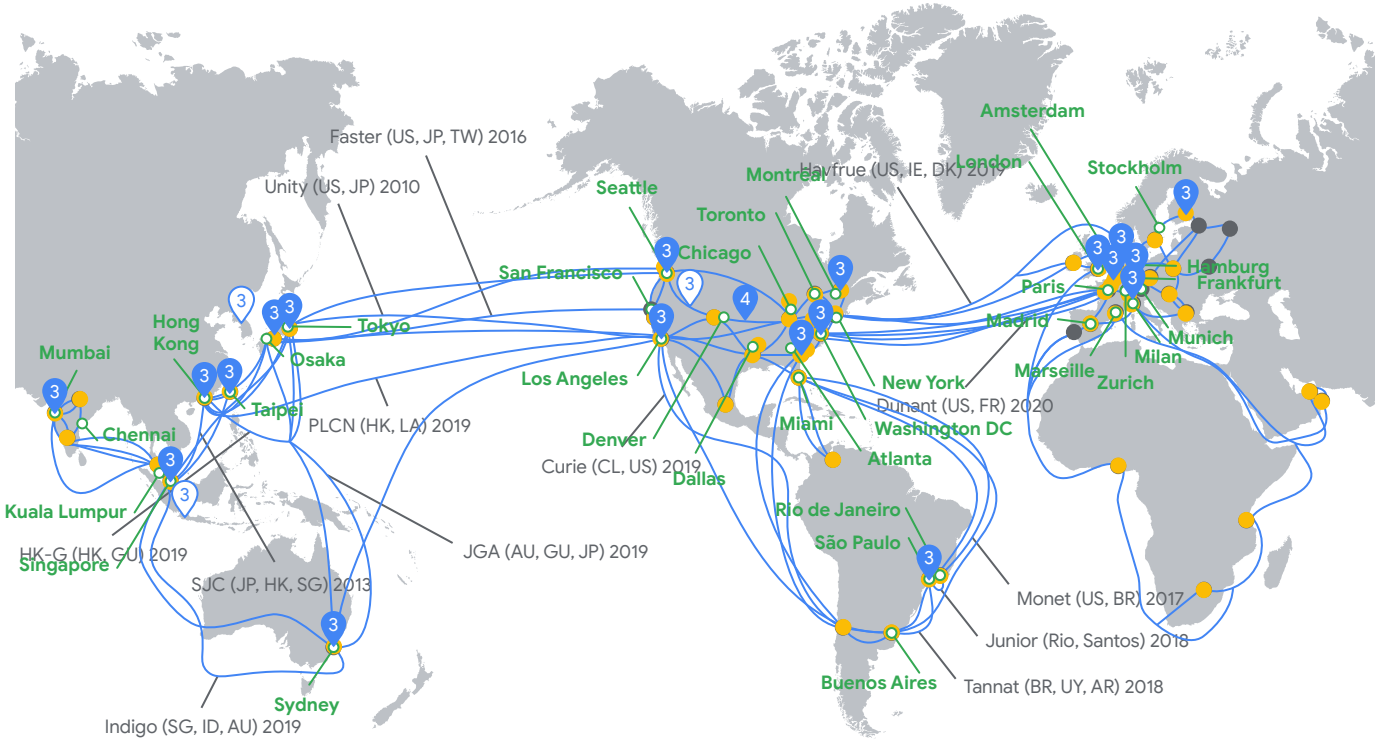
Concrete to Customer

Google Cloud

Google Cloud Platform

Our global infrastructure

- Current regions and number of zones
- Future regions and number of zones
- Edge points of presence
- CDN nodes
- Network
- Dedicated Interconnect



Google Cloud

Defense in depth at scale

- Usage
- Operations
- Deployment
- Application
- Network
- Storage
- OS + IPC
- Boot
- Hardware

Google Cloud

Infrastructure defense against key attack vectors

Usage	Log Auditing	Safe Browsing API	BeyondCorp	Security Key Enforcement		
Operations	Compliance & Certifications	Live Migration Infra maintenance & patching	Threat analysis and intelligence	Open Source Forensics tools	Anomaly Detection (Infrastructure)	Incident Response (Infrastructure)
Deployment	Google Services TLS encryption with perfect forward secrecy	Certificate Authority	Free and automatic certificates	DDoS Mitigation (PaaS & SaaS)		
Application	Peer code review & Static Analysis (Infrastructure SLDC)	Source code/Image provenance (Infrastructure)	Binary authorization (Infrastructure code)	WAF (PaaS & SaaS Use cases)	IDS/ IPS (PaaS & SaaS Use cases)	Web Application Scanner (Google Services)
Network	Infrastructure RPC encryption in transit between data centres	DNS	Global Private Network	Andromeda SDN Controller	Jupiter Datacenter Network	B4 SDN Network
Storage	Encryption at rest	Logging	Identity and Access Management	Global at scale Key Management Service		
OS + IPC	Hardened KVM Hypervisor	Authentication for each host and each job	Curated Host Images	Encryption of Interservice Communications		
Boot	Trusted Boot	Cryptographic Credentials				
Hardware	Purpose-built Chips	Purpose-built Servers	Purpose-built Storage	Purpose-built Network	Purpose-built Data Centers	

Google Cloud

Thanks!

Google Cloud